

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America

v.

STEPHEN LAVERY

Case No.

3:18mj576

MICHAEL J. NEWMAN

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 4/14/2018 and 5/3/2018 in the county of Montgomery in the
Southern District of Ohio, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 2252(a)(2) & (b)(1)

Distribution of child pornography

18 U.S.C. § 2252(a)(4)(B) & (b)(2)

Possession or access with intent to view child pornography

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

Andrea R. Kinzig
 Complainant's signature

Andrea R. Kinzig, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

8/17/18

Michael J. Newman
 Judge's signature

City and state: Dayton, Ohio

Michael J. Newman, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses involving child exploitation and child pornography.
2. Along with other agents, officers, and investigators of the Kettering (Ohio) Police Department, Ohio Bureau of Criminal Investigation (BCI), Cuyahoga County (Ohio) Internet Crimes Against Children (ICAC) Task Force, and FBI, I am currently involved in an investigation of child pornography offenses committed by **STEPHEN LAVERY**. Based on the investigation conducted to-date, there is probable cause to believe that **STEPHEN LAVERY** possessed child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2), and distributed child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). I submit this Affidavit in support of a criminal complaint.
3. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
4. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause that **STEPHEN LAVERY** committed the offenses alleged in the complaint.

BACKGROUND INFORMATION

Pertinent Federal Statutes

5. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempts or conspires to do so.

6. 18 U.S.C. § 2252(a)(2) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
7. For purposes of these statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:
 - a. “Actual or simulated –
 - i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
 - ii. Bestiality;
 - iii. Masturbation;
 - iv. Sadistic or masochistic abuse; or
 - v. Lascivious exhibition of genitals or pubic area of any person.”

Definitions

8. The following definitions apply to this Affidavit:
 - a. “**Child Pornography**” includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. “**Visual depictions**” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. “**Minor**” means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

- d. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- e. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- f. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- g. A **“Forensic Hash”** is the process of using a mathematical function and applying it to a computer file, which results in a **“hash value”**. A **“hash value”** is a unique identifier for the electronic data – similar to a DNA sequence or a fingerprint of the electronic data. When a hash algorithm is used, it computes a string of numbers for a digital file. Any change to the data will result in a change to the hash value. Both MD5 and SHA-1 algorithms are commonly used on forensic image files.

Cloud Storage and Dropbox

9. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
- a. “Cloud” is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. “The cloud” was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.
 - b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
 - c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long-term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router

Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

- d. “Virtual Machine” (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.
 - e. “NetFlow Records” are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.
10. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.’s servers. According to Dropbox Inc.’s privacy policy, at <https://www.dropbox.com/privacy>, Dropbox Inc. collects and stores “the files you upload, download, or access with the Dropbox Service,” and also collects logs: “When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device’s IP address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

Rabb.it

- 11. Rabb.it, commonly referred to as “Rabbit”, operates a video-sharing website that can be accessed at www.rabb.it.com. The website was created in 2013. Rabb.it is currently based in San Mateo, California.
- 12. The Rabb.it application can be downloaded free of charge from the Google Play Store and through Apple iTunes. Users must utilize the Chrome, Firefox, or Opera web browsers to use the application.
- 13. User accounts are created by selecting a user name and providing an email address. Before accounts can be utilized, they must be verified by clicking on a hyperlink in an email sent by the company.

14. The Rabb.it application allows users to watch movies, television, and videos together; video, voice, and message chat with each other; play games together; and browse the Internet together.
15. Users can invite other users into private chat rooms by sending an invite link via email, Facebook, Twitter, or other Rabb.it chat rooms. Once a chatroom is accessed, a list of users are displayed on the right side of the screen in an area with a chat function. There are three main areas in the chat rooms:
 - a. A Rabbitcast, or shared screen, allows users to watch videos or browse the Internet together. It is like a shared Internet browser that anyone inside the room can control.
 - b. Messages, or text chat, allows users to speak to everyone in the room via text messages as well as share images, GIF's, and emoji's.
 - c. Video chat allows users to communicate with each other via web cameras and microphones.

Bing Search Engine

16. Bing is a web search engine owned and operated by Microsoft Corporation, a company based in Redmond, Washington. The search engine can be accessed at www.bing.com.
17. Bing provides a variety of search services, including web, video, image, and map search products. Bing Image is a search engine that allows users to upload images or URL's into the search engine in order to search for other similar images. Users do not need to have a Microsoft account or authenticate their identities in order to use the Bing search services.

NCMEC and CyberTipline Reports

18. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
19. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline.

Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

FACTS SUPPORTING PROBABLE CAUSE

20. In or around January 2015, Dropbox Inc. reported to NCMEC's CyberTipline that approximately four suspected child pornography files were discovered in a Dropbox account associated with the email address goddead145@hotmail.com and a screen or user name of "God Dead". Dropbox Inc. identified that the company discovered the files on or around January 12, 2015. Dropbox Inc.'s records identified that the IP address of 162.234.139.61 (hereinafter referred to as the "TARGET IP ADDRESS") was utilized to log into the Dropbox account during the approximate time period of December 30, 2014 through January 8, 2015.
21. Dropbox Inc. provided the approximately four suspected child pornography files to NCMEC. The files were originally forwarded to the Cuyahoga County ICAC Task Force for further investigation. I later obtained and reviewed these files as part of the investigation. Based on my training and experience, I believe that at least approximately three of the files depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, one of the files is described as follows:
 - a. 2014-08-21_24-19-17_768.mp4: The file is a video that depicts an adult white female performing oral sex on what appears to be a nude toddler-aged white female child. The video is approximately thirty-eight seconds in duration.
22. In or around February 2018, Microsoft Corporation reported to NCMEC's CyberTipline in two separate reports that an individual utilizing the TARGET IP ADDRESS had uploaded two suspected child pornography files to the Bing Images search engine on or around February 14, 2018 and February 15, 2018. The files were originally forwarded to the Cuyahoga County ICAC Task Force for further investigation. I later obtained and reviewed these files as part of the investigation. Based on my training and experience, I believe that at least approximately two of the files depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, one of the files is described as follows:
 - a. 3fcba70b-0dc5-4822-a7df-9d2eedfbbb4d.jpg: The file is an image that depicts what appears to be a nude toddler-aged white female child lying on her back with her legs straddled above her head. What appears to be a penis is next to or touching the child's vagina. The file was uploaded to the Bing Images search engine on or around February 14, 2018.
23. In or around April 2018, Rabb.it reported to NCMEC's CyberTipline via two reports that approximately twenty-two suspected child pornography files were discovered in a Rabb.it account having an account name of "myroomls365". Rabb.it further reported that the account user had a profile name of "Jerkin Hard" and an email address of

shinigamibeasty@gmail.com. Rabb.it's records identified that the twenty-two files were shared on Rabb.it's platform with one or more other users on or around April 14, 2018. Rabb.it's records also identified that the TARGET IP ADDRESS was utilized by the account user at the time the files were shared.

24. Rabb.it provided the approximately twenty-two suspected child pornography files to NCMEC. The files were originally forwarded to the Cuyahoga County ICAC Task Force for further investigation. I later obtained and reviewed these files as part of the investigation. Based on my training and experience, I believe that at least approximately twenty of the files depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, four of the files are described as follows:
- a. 2bf28bb3-b59f-43c8-8fa0-40bd0af4ec76.jpg The file is an image that depicts what appears to be a nude pre-pubescent white female child lying on her back with her legs spread apart. What appears to be an adult white male is kneeling in front of the child and inserting his penis into the child's anus.
 - b. 769634a6-ecaa-4e62-b50e-385fc863fc5b.jpg: The file is an image that depicts what appears to be two pre-pubescent white female children and a nude adult white male on a bed together. What appears to be a nude pre-pubescent white male child and a partially nude adult white female are standing near the bed. One of the female children is holding the penis of the adult male in her hand near her face. The child's mouth is open, and it appears that semen is secreted into her mouth.
 - c. 42b0176f-d7e7-411d-b34f4-1c531f1d679f.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white female child lying in front of a mirror on her back with her legs spread apart, exposing her nude genitals and anus to the camera.
 - d. f595a28f-00cf-4626-9b96-eec94e632611.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white female child lying on her back. A penis is over the child's groin area. There appears to be semen is secreted on the child's abdomen.
25. Pursuant to a search warrant authorized by the United States District Court for the Southern District of Ohio, I obtained from Rabb.it the chat logs which documented how the twenty-two files noted above were shared. These logs identified that the files were shared with two other users in two separate chat rooms on or around April 14, 2018. By way of example, below is an excerpt of one of these chats, which details how the four files described in paragraphs 24(a) through 24(d) were distributed:

Other User: fuk you're trying to make me blow

Jerkin Hard: *Sends the image entitled 2bf28bb3-b59f-43c8-8fa0-40bd0af4ec76.jpg (described in paragraph 24(a))*

Other User: she takesit well

Other User: me too

Jerkin Hard: Getting close here

Jerkin Hard: *Sends the image entitled 769634a6-ecaa-4e62-b50e-385fc863fc5b.jpg (described in paragraph 24(b))*

Other User: Good kiddy slut. Earning that grown up dick

Jerkin Hard: good girl

Other User: *Sends the following image entitled 42b0176f-d7e7-411d-b34f4-1c531f1d679f.jpg (described in paragraph 24(c))*

Other User: *Sends image entitled f595a28f-00cf-4626-9b96-eec94e632611.jpg (described in paragraph 24(d))*

Jerkin Hard: 5 to 11

Other User: Hehe that looks like a fun hole huh?

Jerkin Hard: mm

26. AT&T was identified as the Internet Service Provider for the TARGET IP ADDRESS. On or around April 23, 2018, an investigator from the Cuyahoga County ICAC served a subpoena to AT&T requesting subscriber information for the TARGET IP ADDRESS on the date and time that of one of the suspected child pornography files was shared on the Rabb.it platform. Records received in response to the subpoena identified that the TARGET IP ADDRESS was subscribed to TOMMY LAVERY at 3935 Parliament Place, Apartment 40, Kettering, Ohio. AT&T's records identified that the account was established on or around December 26, 2014.
27. On or around May 2, 2018, a search warrant was authorized by the Kettering (Ohio) Municipal Court for the residence at 3935 Parliament Place, Apartment 40, Kettering, Ohio. Agents and officers of the Kettering Police Department and Ohio BCI executed the search warrant on or around May 3, 2018. Below is a summary of events that transpired during the execution of the search warrant:
- a. When agents and officers arrived, they encountered TOMMY LAVERY and **STEPHEN LAVERY**. TOMMY LAVERY identified that **STEPHEN LAVERY** was his son, and that they lived together at the residence.
 - b. An LG cellular telephone bearing Model LGMS210 was located on **STEPHEN LAVERY**'s person. Various other electronic media were located in the residence during the search. Pursuant to the search warrant, computer examiners from the Ohio BCI conducted forensic previews of these items. Child pornography files were

located on **STEPHEN LAVERY**'s LG cellular telephone but not on any other devices.

- c. After being advised of his Miranda rights, **STEPHEN LAVERY** agreed to be interviewed. **STEPHEN LAVERY** acknowledged that the LG cellular telephone belonged to him. **STEPHEN LAVERY** advised that some time ago, someone had sent him child pornography files in a chat room. **STEPHEN LAVERY** reported that since that time, he had viewed child pornography on his cellular telephone. **STEPHEN LAVERY** thought that he had an addiction to child pornography and needed help.

28. **STEPHEN LAVERY**'s LG cellular telephone was seized and further examined pursuant to the search warrant. This examination revealed the following information (among other information):

- a. More than approximately one thousand image files and more than approximately thirty video files depicting child pornography were recovered from the device (as defined by 18 U.S.C. § 2256(8)). By way of example, five of the files are described as follows:
 - i. TODFUK.mp4: The file is a video that depicts what appears to be a toddler-aged white female child who is nude from the waist down and lying on her back. What appears to be an adult white male engages in anal sexual intercourse with the child. The video is approximately forty-eight seconds in duration.
 - ii. asianfuck.mp4: The file is a video that depicts what appears to be a nude pre-pubescent Asian female child lying on her back. What appears to be an adult white male engages in vaginal sexual intercourse with the child. The video is approximately fourteen seconds in duration.
 - iii. 8iOS_image_upload.jpeg: The file is an image that depicts what appears to be a pre-pubescent white female child lying on her back. The words "FUCK ME" are written on her abdomen above her vagina. What appears to be a penis is inserted into the child's anus. What appears to be another penis is pointed toward and near the child's face.
 - iv. 2DBD3.jpg: The file is an image that depicts what appears to be a nude toddler-aged white female child. What appears to be a penis is in the child's mouth.
 - v. 1521353126256.jpg: The file is an image that depicts what appears to be a pre-pubescent white female child who is nude from the waist down and lying on her back. Her arms and legs are bound together with white tape and white

rope, and white tape is covering her mouth. The child's legs are spread apart, exposing her nude vagina to the camera.

- b. At least approximately seventeen of the image files recovered from the shinigamibeasty@gmail.com Rabb.it account (as reported by Rabb.it to the CyberTipline, as detailed above) and approximately two of the image files uploaded to Bing Images by the TARGET IP ADDRESS (as reported by Microsoft Corporation to the CyberTipline, as detailed above) were recovered from the LG cellular telephone. Some of these files were saved in the active space of the phone, while others were recovered from areas of the phone that save thumbnail images for files viewed on the phone.
 - i. It was noted that the hash values for some of the images did not match the hash values for the files recovered by Rabb.it and Microsoft Corporation. However, the files appear to be the same based on a manual inspection. Based on my training and experience (and as further detailed above in the Background section of the Affidavit), I know that small changes to files – to include converting a file to a thumbnail image – can change the hash value of a file.
- c. A Google account was established on the phone associated with the email address shinigamibeasty@gmail.com (the email address associated with the Rabb.it account).

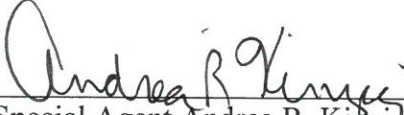
29. Based on all of the information detailed above, there is probable cause to believe that **STEPHEN LAVERY** is the user of the TARGET IP ADDRESS, the shinigamibeasty@gmail.com Rabb.it account, the goddead145@hotmail.com Dropbox account, and the LG cellular telephone. There is also probable cause to believe that **STEPHEN LAVERY** has used his shinigamibeasty@gmail.com Rabb.it account, his goddead145@hotmail.com Dropbox account, the Bing Image search engine, and his LG cellular telephone to possess, access, and distribute child pornography files.

CONCLUSION

30. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that on or around April 14, 2018, **STEPHEN LAVERY**, in the Southern District of Ohio, knowingly distributed any visual depiction using any means or facility of interstate or foreign commerce that has been mailed, shipped and transported in or affecting interstate or foreign commerce, by any means including by computer; and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct, or attempted or conspired to do so, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1).
31. There is also probable cause to believe that on or around May 3, 2018, **STEPHEN LAVERY**, in the Southern District of Ohio, did knowingly possess at least one matter which contains any visual depiction that has been mailed, shipped and transported using any

means and facility of interstate or foreign commerce, including by computer; and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, and such visual depiction was of such conduction, or attempted or conspired to do so, in violation of 2252(a)(4)(B) and (b)(2).

32. I therefore respectfully request that a criminal complaint be granted upon this Affidavit.


Special Agent Andrea R. Kintzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 12th of August 2018


HONORABLE MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

